UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/646,640	11/09/2000	Patrick Salle	00621/TL	1842

41754 7590 07/14/2004

PEHR JANSSON, ATTORNEY AT LAW
7628 PARKVIEW CIRCLE
AUSTIN, TX 78731

EXAMINER	
KIM, JUNG W	

ART UNIT	PAPER NUMBER
2132	8

DATE MAILED: 07/14/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/646,640	SALLE, PATRICK
	Examiner	Art Unit
	Jung W Kim	2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 November 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *18 September 2000*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-8 have been examined. Applicant has amended claims 3-5 and 7-8 in the preliminary amendment filed on November 9, 2000.

Drawings

2. The drawings are objected to under 37 CFR 1.83(a). The drawings must show every feature of the invention specified in the claims. Therefore, the limitations of: 1) the randomly transformed data element being a message block (M, M0, M1, M2, M3) (claim 3), 2) the randomly transformed data element being a message block associated with a key by a logical operator of the exclusive-OR type (claim 4), and 3) a random transformation step preceding the group of operations (270) and the inverse random transformation step following the group of operations (270) (claim 6) must be shown or the feature(s) canceled from the claim(s). No new matter should be entered.

3. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement

sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

4. The title of the invention is not descriptive. A new title is required that is clearly indicative of the invention to which the claims are directed. The following title is suggested: 'Method to prevent power dissipation attacks on a cryptographic algorithm by implementing a random transformation step'.

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claim 1 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim 1 recites the limitation "the random transformation" in line 8. There is insufficient antecedent basis for this limitation in the claim.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Schneier Applied Cryptography 2nd Edition (hereinafter Schneier) in view of Kocher "Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems" (hereinafter Kocher). As per claims 1-4, Schneier teaches a data protection method using a cryptographic algorithm for executing operations for processing data elements (M, M0, M1, M2, M3, K1, K2, K3, K4, K5, R1, R2, R3, R4, R5) so as to generate encrypted information (C) (see Schneier, pages 265-301, DES, especially pages 271-272, Figures 12.1 and 12.2). Although Schneier does not specifically disclose the method being contained in a microprocessor of a chip card, in a different section, Schneier teaches chip cards housing microprocessors that are programmed with different cryptographic protocols (see Schneier, page 587, section 24.13, 'Smart Cards'). It would be obvious to one of ordinary skill in the art at the time the invention was made for the method to be contained in a microprocessor of a chip card since a chip card enables portable but cryptographically secure transaction means as taught by Schneier (see Schneier, page 587, 2nd full paragraph, first sentence and 4th full paragraph, first sentence).

10. Further, Schneier does not disclose a random transform of bits of one of the data elements (K2) by associating a random number with the data element (K2), and after this random transformation step, performing an inverse transformation step (220) such that the encrypted information (C) is unchanged by these transformation steps (120, 220). Kocher teaches a method of using a blinding factor to mask a data element in a cryptographic method, wherein the blinding factor prevents an attacker from observing these data values used in a cryptographic step of this method. A random transform is applied to a data element prior to input of an encryption step and an inverse random transform is applied to the output of the encryption step. This blinding factor leaves the ensuing ciphertext unchanged by the random transformation and its inverse step (see Kocher, page 8, 'Preventing the Attack'). Furthermore, although the random transformation example disclosed by Kocher is a blinding factor specifically using modular multiplication in a public key methodology, the teaching of a blinding factor generalizes to any cryptographic method whenever an attacker can observe a portion of the method (see Kocher, page 1, 'Introduction'; page 8, 3rd full paragraph, second sentence). It would be obvious to one of ordinary skill in the art at the time the invention was made to apply the teaching of Kocher to the method taught by Schneier. Motivation for such a combination enables the method to prevent attacks based on measured observations of certain cryptographic operations of a cryptosystem as taught by Kocher.

11. Further, neither Schneier's teaching of a DES method nor Kocher discloses using an exclusive-OR type operator as the random transformation operator. However,

exclusive-OR operations are the simplest and most basic transforms to mask sensitive data values (see Schneier, pages 13-15, section 1.4, 'Simple XOR'). In addition, as taught by Schneier in a separate section, whitening techniques using the XOR operator in a DES implementation are known means to mask data elements (see Schneier, page 295, 'DESX'; pages 366-367, section 15.6 'Whitening'). It would be obvious to one of ordinary skill in the art at the time the invention was made for the random transform to use a logical operator of the exclusive-OR type. Motivation for such a combination enables the method to implement a basic invertible transformation as the random transformation step in the method taught by Schneier. Finally, the subset of consecutive operations that are commutative in the encryption algorithm taught by Schneier, which allows such a random transformation and its inverse transformation without changing the encrypted information, enables the randomly transformed data element to be any of the following: a key (K1, K2, K3, K4, K5), a message block (M, M0, M1, M2, M3), and/or a message block associated with a key by a logical operator of the exclusive-OR type (R1, R2, R3, R4, R5). The aforementioned covers claims 1-4.

12. As per claim 5, Schneier covers a data protection method as outlined above in the claim 1 rejection. In addition, the cryptographic algorithm for executing operations for processing data comprises a group of operations executed repeatedly (DES has 16 rounds; see Schneier, page 270, 3rd full paragraph).

13. As per claim 6, Schneier covers a data protection method as outlined above in the claim 5 rejection under 35 U.S.C. 103(a). In addition, the random transformation step precedes the group of operations executed repeatedly and the inverse transformation step follows the group of operations (270) (see Schneier, page 272, Figure 12.2; page 366, last paragraph, first sentence).

14. As per claim 7, Schneier covers a data protection method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, Schneier teaches DES variants wherein the order of execution of the operations of the group of operations (27) is randomly modified (see Schneier, page 300, first step).

15. As per claim 8, Schneier covers a data protection method as outlined above in the claim 1 rejection under 35 U.S.C. 103(a). In addition, the cryptographic algorithm is a DES type (see Schneier, pages 265-301, DES).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Akiyama et al. U.S. Patent No. 5,623,548.

Shamir U.S. Patent No. 5,991,415.

Jokobsson U.S. Patent No. 6,049,613.

Curiger et al. U.S. Patent No. 6,064,740.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jung W Kim whose telephone number is (703) 305-8289. The examiner can normally be reached on M-F 9:00-6:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Jung W Kim
Examiner
Art Unit 2132

Jk
July 2, 2004

JUSTIN T. DARROW
PRIMARY EXAMINER